WHAT IS CLAIMED IS:

1. A device, comprising:

at least one interface configured to receive data transmitted via a network;

a firewall configured to:

receive data from the at least one interface,

determine whether the data potentially contains malicious content, and

identify first data in the received data that potentially contains malicious content;

intrusion detection logic configured to:

receive the first data, and

generate report information based on the first data; and

forwarding logic configured to:

receive the report information, and

determine whether to forward the first data for processing by a user application based on the report information.

2. The device of claim 1, wherein the forwarding logic is further configured to:

forward the first data to a user device executing the user application when the determining indicates that the first data does not contain malicious content, and

discard the first data when the determining indicates that the first data contains malicious content.

3. The device of claim 1, wherein the forwarding logic is further configured to:

defer a forwarding decision to a central management system based on parameters associated with the report information, and

forward the report information to the central management system.

4. The device of claim 3, further comprising:

a virtual private network gateway configured to establish a secure connection with the central management system.

5. The device of claim 1, wherein the firewall comprises anti-virus logic configured to examine a data stream for viral signatures using at least one of a signature-based technique, a heuristic technique and a rough set logic technique.

6. The device of claim 5, wherein the anti-virus logic is further configured to identify unsolicited messages.

7. The device of claim 1, further comprising:

a processing device executing the user application, the user application being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files and downloading games.

8. The device of claim 1, wherein at least one of the firewall, the intrusion detection logic and the forwarding logic is configured to receive rule-based processing information from an external device via the network.

9. The device of claim 8, wherein at least one of the firewall, intrusion detection logic and forward logic is further configured to receive updated rule-based processing information from the external device.

10. In a network device configured to receive data transmitted over a network, a method, comprising:

receiving data transmitted via the network;

identifying first data that may contain malicious content;

generating report information based on the first data;

determining, based on the report information, whether to forward the first data for processing by a user device; and

forward the first data to the user device when it is determined that the first data does not contain malicious content.

11. The method of claim 10, further comprising:

forwarding the report information to an external device based on at least one parameter associated with the report information.

12. The method of claim 11, further comprising:

establishing a virtual private network connection to the external device.

13. The method of claim 11, further comprising:

receiving, from the external device, information indicating whether the first data is to be forwarded to the user device; and

dropping the first data when the information indicates that the first data is not to be forwarded.

14. The method of claim 10, wherein the identifying comprises:

examining the received data for viruses using at least one of a signature-based technique, a heuristic technique and a rough set logic-based technique.

15. The method of claim 10, wherein the identifying comprises:

identifying spam.

16. A computer-readable medium having stored thereon a plurality of sequences of instructions, said sequences of instructions including instructions which, when executed by a processor, cause the processor to:

receive data transmitted via a network;

receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data;

determine whether the data may contain malicious content using a first set of rules;

identify first data that may contain malicious content based on the determining; and

determine whether to forward the first data to a user device based on a second set of rules.

17. The computer-readable medium of claim 16, wherein the instructions further cause the processor to:

determine whether the first data contains malicious content based on the second set of rules; and

forward the first data to a user device executing a user application when the determining indicates that the first data does not contain malicious content.

18. The computer-readable medium of claim 16, wherein the instructions further cause the processor to:

defer a forwarding decision to the external device; and

forward information associated with the first data to the external device.

19. The computer-readable medium of claim 18, wherein the instructions further cause the processor to:

establish a virtual private network tunnel with the external device.

20. The computer-readable medium of claim 16, wherein when identifying first data that may contain malicious content, the instructions cause the processor to identify a

virus using at least one of a signature-based technique, a heuristic technique and a rough set logic-based technique.

21. The computer-readable medium of claim 20, wherein when identifying first data that may contain malicious content, the instructions cause the processor to identify spam.

22. The computer-readable medium of claim 16, wherein the instructions further cause the processor to execute the received data, the data being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files and downloading games.

23. A method for providing security information to a plurality of user devices, comprising:

storing, by a security provider, rules-based security information;

providing, by the security provider, a plurality of subscription levels, each subscription level being associated with a different security level and having a different set of rules-based security information; and

downloading, by the security provider, a first set of rules-based security information to a first one of the plurality of user devices, the downloading being performed in response to at least one of a request from the first user device and a subscription associated with the first user device.

24. The method of claim 23, wherein the first set of rules-based security information comprises at least one of firewall-related rules, intrusion detection-related rules and forwarding rules associated with processing data received by the first user device via the Internet.

25. The method of claim 24, wherein the first user device comprise at least one of a network appliance, a set top box, a television-type Internet access device and a computer.

26. The method of claim 23, further comprising:

providing, by the security provider, updated rules-based security information at predetermined intervals.

27. The method of claim 23, further comprising:

receiving, by the security provider, a subscription associated with the first user device, the subscription being associated with a first one of the plurality of subscription levels and wherein the first set of rules-based security information corresponds to the first subscription level.

28. The method of claim 27, wherein the plurality of subscription levels comprises four levels.